

**REMARKS**

This Application has been carefully reviewed in light of the Office Action mailed January 26, 2005. Claims 1-16 were pending in the application. Claims 1-16 were rejected. In order to advance and expedite the prosecution of the present Application, Applicants amend Claim 10. Thus, Claims 1-16 remain pending in the Application.

In the Office Action, the following actions were taken or matters were raised:

**SPECIFICATION OBJECTIONS:**

The specification was objected to for informalities. The Examiner suggested that Applicants provide the serial numbers of all co-pending applications mentioned on page 1 of the disclosure. Applicants have amended pages 1-3 of the specification to include the serial numbers of the respective noted co-pending applications.

Further, the Examiner suggested that the Title be removed from the abstract page of the specification. Applicants have so amended the abstract page of the specification to remove the Title therefrom. Accordingly, Applicants respectfully request that these objections now be withdrawn.

**SECTION 102 REJECTIONS**

Claim 10 was rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,704,874 issued to Porrás (hereinafter "*Porrás*"). Applicant respectfully traverses this rejection.

Applicants respectfully submit that *Porrás* does not disclose or even suggest each and every limitation of independent Claim 10 as amended. For example, Applicants respectfully submit that *Porrás* does not disclose or even suggest "identifying, by an intrusion detection application, a frame of data as intrusion-related" and "decoding, by the intrusion detection application, the intrusion-related data" as recited by amended Claim 10.

*Porrás* appears to disclose a monitoring system 22 having, for example, an intrusion detection system (*Porrás*, column 3, lines 30-32, figure 1). *Porrás* also appears to disclose that the monitoring system 22 of *Porrás* produces an alert stream that is sent via a secure electronic communication line (SSL) 30 to an alert manager 24 for collection, processing and distribution (*Porrás*, column 3, lines 34-37, lines 62-67, figure 1). *Porrás* further appears to disclose that the alert manager 24 of *Porrás* is equipped with a translation module 32 to translate original, raw data

streams received from the monitors 22 into a common format for further processing (*Porras*, column 4, lines 6-10). Thus, the *Porras* system does not appear to disclose or even suggest having an intrusion detection application for “identifying . . . a frame of data as intrusion-related” and “decoding . . . the intrusion-related data” as recited by amended Claim 10. To the contrary, the intrusion detection system of *Porras* (monitoring system 22 of *Porras*) does not appear to perform any decoding and/or translating function to the raw data streams generated thereby. Accordingly, for at least this reason, Applicants respectfully submit that *Porras* does not anticipate amended Claim 10.

### **SECTION 103 REJECTIONS**

Claims 1-9 and 11-16 were rejected under 35 U.S.C. 103(a) as being unpatentable over *Porras* and further in view of U.S. Patent No. 6,453,345 issued to Trcka et al. (hereinafter “*Trcka*”). Claims 11-13 are rejected under 35 U.S.C. §103(a) as being unpatentable over *Porras*, as applied to claim 10, and further in view of *Trcka*. Applicants respectfully traverse these rejections.


Of the rejected claims, Claim 1 is independent having Claims 2-9 depending therefrom. Further, rejected Claims 11-16 depend from independent Claim 10. Independent Claim 1 recites, at least in part, “decoding the event-data by a decode engine, the decode engine integrated within the intrusion detection application” (emphasis added). As discussed above in connection with independent Claim 10, *Porras* does not disclose or even suggest a “decode engine integrated within the intrusion detection application” as recited by independent Claim 1 (emphasis added). To the contrary, as discussed above, the “translating module 32” of *Porras* referred to by the Examiner in the Office Action (page 4) is remote from the intrusion detection system (monitoring system 22) of *Porras*. Further, *Trcka* does not remedy the deficiencies of *Porras* in at least this regard. Accordingly, the proposed combination of the *Porras* and *Trcka* references, alone or in combination, does not disclose, teach or suggest each and every limitation of either of independent Claims 1 and 10. Accordingly, Claims 1-9 and 11-16 are in condition for allowance, and Applicants respectfully requests that the rejection of Claims 1-9 and 11-16 be withdrawn.

**CONCLUSION**

Applicants have made an earnest attempt to place this case in condition for immediate allowance. For the foregoing reasons and for other reasons clearly apparent, Applicants respectfully request reconsideration and full allowance of all pending claims.

No fee is believed due with this Response. If, however, Applicants have overlooked the need for any fee due with this Response, the Commissioner is hereby authorized to charge any fees or credit any overpayment associated with this Response to Deposit Account No. 08-2025 of Hewlett-Packard Company.

Respectfully submitted,

By:   
James L. Baudino  
Reg. No. 43,486

Date: April 21, 2005

Correspondence to:  
L.Joy Griebenow  
Hewlett-Packard Company  
Intellectual Property Administration  
P. O. Box 272400  
Fort Collins, CO 80527-2400  
Tel. 970-898-3884